

AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("—") being deleted:

1. (Currently Amended) A computer security system, comprising:

a processor; and

a memory component that stores:

a security module adapted to control access to a secure computer resource by a user via a client based on verification of a security credential provided by the user; and verification data disposed on the client and accessible by the security module, the security module adapted to enable the user to recover the security credential from the client based on a response received from the user associated with the verification data.

2. (Original) The system of Claim 1, wherein the security module is adapted to enable the user to reset the security credential based on the response.

3. (Original) The system of Claim 1, wherein the security module is adapted to generate a query to present to the user based on the verification data.

4. (Original) The system of Claim 1, wherein the security module is adapted to control booting of the client based on the response.

5. (Original) The system of Claim 1, wherein the security module is adapted to initiate a collection module to acquire the verification data from the user.

6. (Original) The system of Claim 1, wherein the security module is adapted to encrypt the security credential based on the verification data.
7. (Original) The system of Claim 1, wherein the security module is adapted to decrypt an encrypted security credential based on the response.
8. (Original) The system of Claim 1, wherein the security module is disposed in a basic input/output system (BIOS).
9. (Original) The system of Claim 1, wherein the security module is adapted to control access to a secure communications network.
10. (Original) The system of Claim 1, wherein the security module is adapted to control access to a computer network resource.
11. (Original) The system of Claim 1, wherein the security module is adapted to enable the user to retrieve the security credential based on the response.
12. (Original) The system of Claim 1, wherein the security module is adapted to automatically reset the security credential based on the response.
13. (Original) the system of Claim 1, wherein the security module is disposed on the client.

14. (Previously Presented) A computer security system, comprising:
means for controlling access to a secure computer resource associated with a client
based on verification of a security credential provided by a user of the client; and
means for accessing verification data disposed on the client to enable the user to
recover the security credential based on a response received from the user via the controlling
means.

15. (Previously Presented) The system of Claim 14, wherein the means for
accessing comprises means for generating a query presentable to the user.

16. (Original) The system of Claim 14, wherein the controlling means comprises
means for controlling booting of the client based on the response.

17. (Original) The system of Claim 14, further comprising means for initiating a
collection module for acquiring verification data from the user.

18. (Original) The system of Claim 14, further comprising means for automatically
resetting the security credential based on the response.

19. (Currently Amended) A computer security method, comprising:
receiving a request at a client to access a secure computer resource, a security credential required from a user to access the secure computer resource;
presenting verification data disposed on the client to the user; and
enabling the user to recover the security credential from the client based on a response received from the user to the verification data.

20. (Original) The method of Claim 19, further comprising initiating booting of the client based on the response.

21. (Original) The method of Claim 19, wherein presenting the verification data comprises generating a query to present to the user for recovery of the security credential.

22. (Original) The method of Claim 19, wherein enabling the user to recover the security credential comprises enabling the user to reset the security credential based on the response.

23. (Original) The method of Claim 19, further comprising initiating a collection module to acquire the verification data from the user.

24. (Original) The method of Claim 19, further comprising encrypting the security credential based on the response received from the user to the verification data.

25. (Original) The method of Claim 19, further comprising decrypting an encrypted security credential based on the response received from the user to the verification data.

26. (Original) The method of Claim 19, further comprising receiving the response to a query presented to the user for recovery of the security credential.

27. (Original) The method of Claim 19, further comprising accessing a secure computer communications network based on the response.

28. (Original) The method of Claim 19, further comprising accessing a secure computer network resource based on the response.

29. (Original) The method of Claim 19, wherein enabling the user to recover the security credential comprises enabling the user to retrieve the security credential based on the response.

30. (Original) The method of Claim 19, wherein enabling the user to recover the security credential comprises automatically resetting the security credential for the user based on the response.

31. (Currently Amended) A computer security system, comprising:

a processor; and

a memory component that stores:

a collection module adapted to receive and store verification data associated with a user on a client; and

a recovery module adapted to enable the user to recover from the client a security credential associated with accessing a secure computer resource via the client by verifying the user response to the verification data.

32. (Original) The system of Claim 31, wherein the recovery module is adapted to generate a query presentable to the user based on the verification data.

33. (Original) The system of Claim 31, wherein the recovery module is adapted to enable the user to reset the security credential.

34. (Original) The system of Claim 31, wherein the recovery module is disposed within a basic input/output system (BIOS).

35. (Original) The system of Claim 31, further comprising an encryption/decryption module adapted to encrypt the security credential using the verification data.

36. (Original) The system of Claim 31, further comprising an encryption/decryption module adapted to decrypt the security credential based on the response.

37. (Original) The system of Claim 31, wherein the recovery module is adapted to enable the user to retrieve the security credential.

38. (Original) The system of Claim 31, wherein the recovery module is adapted to automatically reset the security credential for the user based on the user response.

39. (Original) The system of Claim 31, wherein the recovery module is disposed on the client.

40. (Currently Amended) A computing device, comprising:

a processor; and

a memory component that stores:

a security module disposed on the computing device and configured to control access to a secure computer resource associated with the computing device based on authentication of a security credential; and

a recovery module disposed on the computing device and configured to enable a user to retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device.

41. (Previously Presented) The device of Claim 40, wherein the recovery module enables a user to independently retrieve the security credential.

42. (Previously Presented) The device of Claim 40, wherein the recovery module enables a user to independently reset the security credential.

43. (Previously Presented) The device of Claim 40, wherein the recovery module automatically resets the security credential for the user in response to retrieving the security credential.

44. (Previously Presented) The device of Claim 40, wherein the recovery module is configured to retrieve the security credential based on a response received from the user associated with the verification data.

45. (Previously Presented) The device of Claim 40, wherein the verification data comprises data associated with a query and response mechanism.

46. (Previously Presented) The device of Claim 40, wherein the security module is disposed in a basic input/output system (BIOS).